CLAIMS

What is claimed is:

Sub a4

1. An apparatus for providing a computer security firewall, comprising:

an ASIC including a firewall engine with a first engine including a first set of rules for sorting incoming IP packets into initially allowed packets and initially denied packets, and a filter including a second set of rules for receiving and further sorting the initially denied packets into allowed packets and denied packets.

2. The apparatus of claim 1, wherein the filter dynamically generates the second set of rules.

3. The apparatus of claim 2, wherein the first set of rules comprises fixed rules.

4. The apparatus of claim 3, further comprising:

a second engine for receiving and further processing the initially allowed packets.

5. The apparatus of claim 4, wherein the second engine is capable of modifying some subset of the initially allowed packets.

6. The apparatus of claim 5, wherein the second engine comprises a dynamic analyzer for identifying initially allowed packets requiring network address translation, and a handler for providing network address translation.

7. The apparatus of claim 5, wherein the second engine comprises a dynamic analyzer for sending a "reset" packet to a source IP address.

8. A computer software product for providing a network security firewall, comprising:

computer code for sorting incoming IP packets into initially allowed packets and initially denied packets;

computer code for extracting matching criteria from incoming IP packets;

computer code for dynamically generating rules using the extracted matching criteria; and

computer code for further sorting the initially denied packets using the dynamically-generated rules.

9. The computer software product of claim 8, wherein the computer code for sorting incoming IP packets uses fixed rules.

10. The computer software product of claim 9, further comprising:

computer code for further sorting the initially allowed packets into allowed packets and packets requiring modification.

11. The computer software product of claim 10, further comprising computer code for modifying control packets.

12. The computer software product of claim 11, wherein the computer code for modifying control packets includes computer code for network address translation.

13. The computer software product of claim 10, further comprising:

computer code for generating and transmitting a "reset" packet in response to a denied packet.

14. A method for providing network computer security, comprising:

receiving incoming IP packets at a firewall;

sorting the incoming IP packets into initially allowed packets and initially denied packets; and

further sorting the initially denied packets into allowed and denied packets using dynamically-generated rules.

15. The method of claim 14, wherein the step of sorting the incoming IP packets is performed using fixed rules.

16. The method of claim 15, further comprising the step of further sorting the initially allowed packets into allowed packets and packets requiring modification.

17. The method of claim 16, further comprising the step of providing network address translation for packets requiring modification.

18. A method for providing network computer security, comprising:

receiving incoming IP packets at a firewall;

sorting the incoming IP packets into initially allowed packets and initially denied packets using a set of fixed rules;

extracting parameters from the incoming IP packets;

using the extracted parameters to generate a set of dynamically-generated rules; and

further sorting the initially denied packets into allowed and denied packets using the dynamically-generated rules.

19. The method of claim 18, further comprising the step of further sorting the initially allowed packets into allowed packets and packets requiring modification.

20. The method of claim 19, further comprising the step of providing network address translation for packets requiring modification.